CMMC Update:
Review of NIST 800-171 Rev3

Current As Of: June 2023

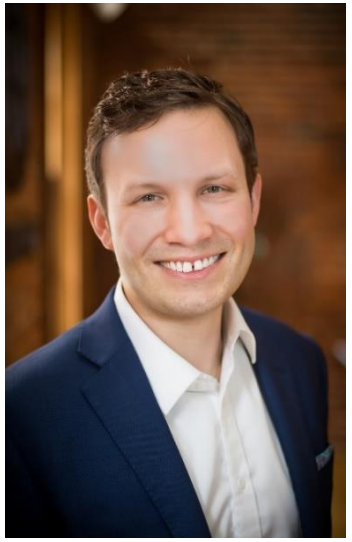
Sponsored by:
COALFIRE FEDERAL

TODAY'S SPEAKERS

Amira Armond

President

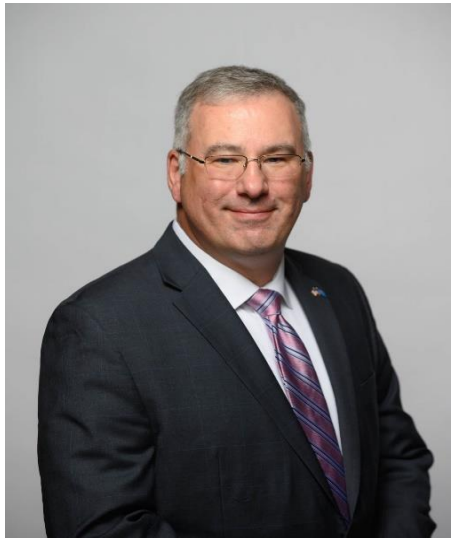
Kieri Solutions
Vice Chair, C3PAO Stakeholder Forum



Ryan Heidorn

Chief Technology Officer

C3 Integrated Solutions
Board Director, NDIA New England



Vince Scott

CEO

Defense Cybersecurity Group
INFRAGARD National SME Cyberwarfare

Sponsored by:

Secure Your Networks and Systems In Physical Space and Cyberspace

- **Secure your Networks. Now**
- Contractual obligation to comply with National Institute of Standards and Technology (NIST) 800-171Rev2
  - Companies not complying sufficiently under current regulation
  - Does not negate obligation to meet the contractual requirements
- CMMC announced Jul ’19 -- 3rd Party Assessments to ensure 800-171 implementation in the future
  - CMMC 2.0 announced Nov ’21
- **DRAFT NIST 800-171Rev3 released 10 May 23**

Overview of Changes to NIST 800-171 Rev3

- **Why do we care?**
  - NIST 800-171 establishes the security requirements/controls contractors must implement if the contractor processes, handles, or store Controlled Unclassified Information (CUI)
- **What changed?**
  - 3 new Domains: **Planning**, **System and Service Acquisition**, **Supply Chain Risk Management**
  - Still lists 110 requirements but many now multi-part
    - Result: additional requirements…depending on your counting method ~270
  - 5 requirements eliminated
  - Introduction of "***Organizationally Defined Parameters***"
- **DRAFT comment period ends 14 Jul 23**

Impact relative to CMMC

- **Based on changing timelines, government will implement NIST Rev3 prior to DoD implementing CMMC 3rd Party Assessments**
  - Per DoD CISO, DoD now “targeting” late fall 24 for CMMC final rule
  - NIST plans a second Rev3 draft in Oct 24 / Final NLT Feb 24
  - Rev3 the standard 1 year or longer prior to CMMC assessments
- **CMMC assessment guides based on Rev2 -- will require modification or cancellation**
  - CAP will require major revision based on new DFARS Rule, but scoping guide should not require revision

Organization-Defined Parameters (ODPs)

- **ODP concept introduced from NIST SP 800-53**
- **ODPs are positioned in the 800-171 Rev3 draft as providing** "flexibility… to specify values for the designated parameters, as needed."
- **Example:**

> **3.1.8. Unsuccessful Logon Attempts**
>
> Limit the number of consecutive invalid logon attempts by a user to [*Assignment: organization-defined number*] in [*Assignment: organization-defined time period*].

ODPs: Unsuccessful Login Attempts

800-171 Rev2

3.1.8 **Limit unsuccessful logon attempts.**

800-171 Rev3 ipd

3.1.8. Unsuccessful Logon Attempts

Limit the number of consecutive invalid logon attempts by a user to [*Assignment: organization-defined number*] in [*Assignment: organization-defined time period*].

800-53 Rev5

AC-7 **UNSUCCESSFUL LOGON ATTEMPTS**

Control:

a. Enforce a limit of [*Assignment: organization-defined number*] consecutive invalid logon attempts by a user during a [*Assignment: organization-defined time period*]; and

b. Automatically [*Selection (one or more): lock the account or node for an [Assignment: organization-defined time period]; lock the account or node until released by an administrator; delay next logon prompt per [Assignment: organization-defined delay algorithm]; notify system administrator; take other [Assignment: organization-defined action]*] when the maximum number of unsuccessful attempts is exceeded.

Who Defines ODPs?

- **There are 117 ODPs in 800-171 Rev3 draft**
- **Who is the "organization" that defines the ODPs?**
  - "These ODPs provide additional flexibility by allowing **federal organizations** to specify values for the designated parameters, as needed." – NIST SP 800-171 Rev3 ipd
  - "Determination of the organization-defined parameters can evolve from many sources, including laws, executive orders, directives, regulations, policies, standards, guidance, and mission or business needs." – NIST SP 800-53 Rev5

Who Define ODPs?

- **“We don’t know who will step forward and fill that organizational role at this point in time.”** – Dr. Ron Ross, June 6, 2022

- **For CUI Basic (“CUI”)**
  - NARA (ISSO) as CUI Executive Agent; **then,**
  - Federal agencies such as DoD, when used in contractual vehicles with nonfederal organizations; **then,**
  - Nonfederal organizations

- **For CUI Specified**
  - Governed by the relevant Safeguarding and/or Dissemination Authority, if applicable; **then,**
  - Nonfederal organizations

- **What happens when multiple agencies specify different ODPs?**

ODP Specification in Action

800-53 Rev5

AC-7 UNSUCCESSFUL LOGON ATTEMPTS

Control:

a. Enforce a limit of [*Assignment: organization-defined number*] consecutive invalid logon attempts by a user during a [*Assignment: organization-defined time period*]; and

b. Automatically [*Selection (one or more): lock the account or node for an [Assignment: organization-defined time period]; lock the account or node until released by an administrator; delay next logon prompt per [Assignment: organization-defined delay algorithm]; notify system administrator; take other [Assignment: organization-defined action]]* when the maximum number of unsuccessful attempts is exceeded.

FedRAMP Moderate Baseline SSP Template

AC-7 Unsuccessful Login Attempts (L) (M)

The organization:

(a) Enforces a limit of [*FedRAMP Assignment: not more than three (3)*] consecutive invalid logon attempts by a user during a [*FedRAMP Assignment: fifteen (15) minutes*]; and

Automatically [*Selection: locks the account/node for a [FedRAMP Assignment: thirty (30) minutes]; delays next logon prompt according to [Assignment: organization-defined delay algorithm]]* when the maximum number of unsuccessful attempts is exceeded.

Hypothetical DoD Assignment of ODPs

800-171 Rev3 ipd

3.13.11. Cryptographic Protection

Implement the following types of cryptography when used to protect the confidentiality of CUI: [*Assignment: organization-defined types of cryptography*].

Hypothetical Specification of ODP

3.13.11. Cryptographic Protection *EXAMPLE ONLY*

Implement the following types of cryptography when used to protect the confidentiality of CUI: ***[DoD Assignment: FIPS-validated or NSA-approved cryptography]***

3.4.8 Authorized Software

800-171 Rev3 ipd

3.4.8. Authorized Software – Allow by Exception

a. Identify software programs authorized to execute on the system.

b. Implement a deny-all, allow-by-exception policy to allow the execution of authorized software programs on the system.

c. Review and update the list of authorized software programs [*Assignment: organization-defined frequency*].

800-171 Rev2

3.4.8 **Apply ~~deny-by-exception (blacklisting) policy to prevent the use of unauthorized software~~ or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.**

3.13.7 Split Tunneling

800-171 Rev3 ipd

3.13.7. Split Tunneling

Prevent split tunneling for remote devices unless the split tunnel is securely provisioned using [*Assignment: organization-defined safeguards*].

800-171 Rev2

3.13.7 **Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).**

3.13.11 Cryptographic Protection

800-171 Rev3 ipd

3.13.11. Cryptographic Protection

Implement the following types of cryptography when used to protect the confidentiality of CUI: [*Assignment: organization-defined types of cryptography*].

800-171 Rev2

3.13.11 Employ ~~FIPS-validated cryptography~~ when used to protect the confidentiality of CUI.

FIPS is dead. Long live FIPS?

Sponsored by:

3.13.17 Internal Network Communications Traffic

800-171 Rev3 ipd (NEW)

3.13.17. Internal Network Communications Traffic

Route internal network communications traffic to external networks through an authenticated proxy server.

- Derived from NIST 800-53 Rev5, SC-7(8)
  In 800-53, the control enhancement has an ODP for *organization-defined internal traffic* going to *organization-defined external networks*. In 800-171 Rev3 ipd, the requirement seems to be for all internal network communications traffic to all external networks.

- Aligns well with the move to zero trust architecture (ZTA); this requirement could be met by ZTA technologies such as a secure web gateway (SWG), security service edge (SSE) technologies, or other zero trust network access (ZTNA) technologies.

Withdrawn (…And Not Reincorporated)

- **3.5.6 Disable identifiers after a defined period of inactivity.**
- **3.5.8 Prohibit password reuse for a specified number of generations.**
- **3.7.1 Perform maintenance on organizational systems.**
- **3.13.14 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.**
- **3.14.5 Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.**
- **22 other requirements in NIST SP 800-171 Rev2 were reincorporated into other controls in 800-171 Rev3 ipd. *Those 22 requirements are still present in Rev3.***

Reincorporated Requirements

SP 800-171r2

3.10.3 **Escort visitors and monitor visitor activity.**

DISCUSSION

Individuals with permanent physical access authorization credentials are not considered visitors. Audit logs can be used to monitor visitor activity.

3.10.4 **Maintain audit logs of physical access.**

3.10.5 **Control and manage physical access devices.**

SP 800-171r3 IPD

1530 **3.10.7. Physical Access Control**

1531 1532 a. Enforce physical access authorizations at [*Assignment: organization-defined entry and exit points to the facility where the system resides*] by:

1533 1. Verifying individual access authorizations before granting access to the facility; and

1534 1535 1536 2. Controlling ingress and egress to the facility using [*Selection (one or more): [Assignment: organization-defined physical access control systems or devices]; guards*].

1537 1538 b. Maintain physical access audit logs for [*Assignment: organization-defined entry or exit points*].

1539 1540 c. Escort visitors and control visitor activity [*Assignment: organization-defined circumstances requiring visitor escorts and control of visitor activity*].

1541 d. Secure keys, combinations, and other physical access devices.

1512 **3.10.3.** Withdrawn: Incorporated into 3.10.7.

1513 **3.10.4.** Withdrawn: Incorporated into 3.10.7.

1514 **3.10.5.** Withdrawn: Incorporated into 3.10.7.

Graphic from “Making Sense of 171r3”, presented by Jacob Horne at the NDIA New England Cyber Event, May 10, 2023. Used with permission.

Secure Your Networks and Systems In Physical Space and Cyberspace

- **Secure your Networks. Now**
- **Know your contracts**
- **Know your business processes**
  - Cybersecurity is an operational imperative, not an IT problem
- **Based on your contracts and processes, implement the biggest impact/biggest value solutions**
- **ISO 27001 Certification?**
- **Comments on R3? membership@ndia.org by 4 July for consolidation prior to the 14 July deadline**

Questions?

Sponsored by:

NFOs and SCRM

- **Most NFO controls/requirements (see Appendix E of 171Rev2… these are assumed to be in place) were incorporated into the main body although a few remain**
- **Policies and Procedures now explicitly required as part of the new Planning Domain**
  - They did not break this down for each domain and do ***not*** require a procedure for each requirement
  - “Procedures can be documented in system security plans or in one or more separate documents.”
- **Supply Chain Risk Management (SCRM)**
  - “**Develop a plan** for managing supply chain risks associated with the development, manufacturing, acquisition, delivery, operations, maintenance, and disposal of the system, system components, or system services. “

External systems and supply chain

- **Addresses major flaw of Rev2**
  - **Verifying security of external systems was barely mentioned – and no minimums defined**
    - Cloud hosting providers: AWS, Office 365, SalesForce
    - Service providers: Remote Management clouds, MSPs, MSSPs
    - Other providers: Co-locations, third party datacenters, consultants
- **Flaw drove DoD to add extra requirement: “clouds must be FedRAMP moderate or equivalent”**
  - Will Rev3 clarify expectation is 800-171 for non-federal systems?

Use of External Systems

- **<u>Goal</u>: If an external information system can access your CUI, make sure it is at least as secure as your information system!**

- **3.1.20:** [Selection (one or more): Establish [Assignment: organization-defined terms and conditions]; **Identify** [Assignment: **organization-defined controls asserted to be implemented on external systems**]], consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:
  1. Access the system from external systems; and
  2. Process, store, or transmit CUI using external systems; **OR** b. Prohibit the use of [Assignment: organizationally-defined types of external systems].
- **3.1.21:** a. Permit authorized individuals to **use an external system** to **access the system** or to **process, store, or transmit CUI** only after:
  1. Implemented **controls on the external system** as specified in the organization's security policies and security plans **are verified**; or
  2. Approved system connection or processing **agreements** with the organizational entity hosting the external system **are retained**.

External service providers

- **Goals**:
  - Know how your provider is helping you perform security requirements
  - Ensure they perform appropriate controls
  - Evaluate regularly
- a. Require the providers of external system services to **comply with organizational security requirements**, and implement the following controls: [Assignment: **organization-defined controls].**
- b. Define and document organizational oversight and user roles and responsibilities with regard to external system services.
- c. Implement the following processes, methods, and techniques to **monitor control compliance by external service providers on an ongoing basis:** [Assignment: organization-defined processes, methods, and techniques]

Supply Chain Risk Management Domain

- **Goals:**
  - Prevent purchase of pre-compromised materials (backdoor chips added to motherboards)
  - Avoid counterfeit parts (Cisco)
  - Reduce risk of product/service becoming compromised (Solarwinds)
  - Reduce risk of risk of product/service not performing its purpose (MSSPs that fail to perform incident monitoring)
- **Different from contractual SCRM which focuses on not passing-through compromised / counterfeit parts to US Government**

Independent assessment requirements

- **3.12.5. Independent Assessment**
  - Use independent assessors or assessment teams to assess controls
- **Independent assessors or assessment teams**
  - Individuals or groups who conduct impartial security assessments of the system
  - “Impartiality” means assessors are free from perceived or actual conflicts of interest regarding development, operation, sustainment, or management of the system under assessment or the determination of control effectiveness.

NDIA Recommendations

1. **DoD CIO include industry in their assessment plan**
   - Focus on “How” and “What”
   - Understand cost impact on SMBs below the cybersecurity poverty line
2. **“How” – Adjust implementation plan**
   - Assess MSPs as part of a cohesive strategy; verify providers meet standards on behalf of their clients
   - Identify controls assessors can identify for immediate correction
   - Limit controls that drive automatic fail
3. **“What” – Limit scope of material for protection**
   - Require senior leader approval